DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
CNATRA
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CNATRAINST 5230.6A
N6
01 AUG 2005

CNATRA INSTRUCTION 5230.6A

Subj: CNATRA POLICY AND GUIDELINES FOR PASSWORD AUTHENTICATION WHEN USING DON INFORMATION SYSTEMS (IS) RESOURCES OR USING INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY (IMIT) ASSETS

Ref: (a) CNATRAINST 5000.2C (R
(b) CNATRAINST 5200.7B (R
(c) DODI 5200.40
(d) DODI 8500.2
(e) DODD 8000.1
(f) DODD 8500.1
(g) CJCSM 6510.01
(h) OPNAVINST 5239.1B

Encl: (1) List of Web Links to References

1. Purpose

a. To provide a policy, and guidelines for Chief of Naval Air Training (CNATRA) and Naval Air Training Command (NATRACOM) units user's data access on CNATRA unclassified assets residing on the web or respective central databases. This data is unclassified but sensitive and is protected and controlled on a need-to-know basis by System Administrators (SA) or Network Administrators (NA) User Identifications (USERID) accounts and passwords to respective users.

b. To define the organizational structure of the policy and guidelines.

c. To issue policy and guidelines necessary for consistent and effective implementation throughout CNATRA and NATRACOM.

d. To apply basic policy, principles of administrative guidelines as they relate to Information Management and Information Technology (IMIT) and Information Systems (IS) associated with and connected to the CNATRA and NATRACOM Databases and Networks.

A) 2. Cancellation: CNATRAINST 5230.6 and NRSINST 5230.5. The focus of this revision is to separate the joint CNATRA/NRS instruction. The only revision markings used are to show other modifications.

3. Objective. To provide Command policy and guidelines for CNATRA System Administrators (SA) and Network Administrators (NA) in administrating and managing user accounts and passwords for users on unclassified networks or central databases at CNATRA and NATRACOM units for personnel in support of database access, maintenance, programming support of legacy systems, under the purview of the CNATRA Command Information Officer (CIO).

4. Authority. The CNATRA Command Information Officer (CIO) is responsible for ensuring compliance with DOD and DON Information Management and Information Technology (IMIT) policies and guidance for Information Systems (IS). Reference (a) identifies this authority. Reference (b) identifies Information Assurance (IA) Program for Information Security (INFOSEC) guidelines. Reference (c) covers the DOD Information Technology Security Certification and Accreditation Process (DITSCAP). Reference (d) provides Information Assurance implementation guidelines and policies. Reference (e) includes the Management of DOD Information Resources and Information Technology. Reference (f) provides specific guidelines for Information Assurance policies. Reference (g) (For Official Use Only (FOUO)) manual provides additional interactive understanding between directives, instructions and guidelines for establishing this password policy. Reference (h) is the Navy Information Assurance (IA) Program. The policies, guidelines and principles presented in references (a) through (h) and this instruction apply to all personnel at CNATRA and NATRACOM military, Government civilian, (including Government contractors and International Military Training Personnel) who use IMIT resources or provide support to Information Systems (IS) within CNATRA and NATRACOM units. Enclosure (1) is a list of web links

R) to references. NETWARCOM/N6 has CIO and DAA responsibilities for NMCI. CNATRA CIO is the DAA and has DAA responsibilities for all Legacy systems.

D)

5. Policy

a. The term User Identification (USERID) and password identify a unique convention and method to protect unclassified but sensitive data or databases before accessing into a protected unclassified system or on the web. Access to DON Information Systems (IS) or networks is a revocable privilege.

Authentication of User Identification (USERID) and password are covered in specific guidelines and procedures in paragraph 5 below of this instruction. Initial USERID and password or user accounts are provided to a user by a System Administrator (SA), Network Administrator (NA), Security Manager (SM) or, if SA/NA are not available, an Activity Customer Technical Representative (ACTR). Inactivity or not logging onto the data or database by a user for a certain consecutive period of time, normally 90 days, will preempt the user from accessing into the system and require a new USERID account and password from respective database System Administrators (SA) or Network Administrators (NA). In addition, incorrect logons after three (3) unsuccessful attempts will lock the system, preempt the user from accessing the system and will require a system reset by respective SA or NA. Note that the term System Administrators (SA) or Network Administrators (NA) are used interchangeably in this instruction, depending on context of access in a database or Network.

b. Implementation Guidelines for USER IDs and passwords:

(1) Authentication. Outlines minimum implementation requirements for authentication of individual users on DOD information systems. The SA or NA authenticates user access through a unique User Identification (USERID) and password. The user gains access to respective systems with a minimum of a USERID and authenticator. An authenticator may be something the user knows (password), something the user possesses (token), or a physical characteristic (biometric). The most common authenticator is a password. Users are required to login with USERID and password to authenticate themselves before access is granted to the system. Password-protected screen savers should be used if available on system. Initially, a user will receive a permanent USERID and temporary password from the SA or NA, then the user creates one that he or she will memorize. Anonymous/group accounts are prohibited.

(2) Password Ownership. A personal password, not a system level password, will be individually owned, rather than owned in common by a group of individuals to provide individual accountability within a system.

(3) Individual ownership of personal passwords is required to:

(a) Establish individual accountability to determine who accessed what resources, when, and for what purposes.

(b) Establish illicit use of a password or loss of password.

(c) Be used for an audit trail of the activities of a user.

(d) Avoid the need to change the password of an entire group when a single member of the group leaves or loses authorization privileges.

(e) When possible, use a password enforcement program to verify a password that complies with the password policy. For student courseware or other web on-line access, it will be tailored to the length of the student's physical stay in the unit and access removed upon termination of individual's duty or PCS.

(f) Passwords are linked to personal accounts with varying levels of access. Personnel granted authorized access to DOD computer systems or networks will not share passwords or account access. This includes supervised or unsupervised usage by personnel not assigned to the account.

(4) Password Format. Passwords will be at least eight characters long and consist of a mix of uppercase letters, lowercases letters, numbers, and special characters, using three or four character sets. Note: Eight characters are the DOD minimum requirement. If technically feasible, 12 to 16 characters using a mix of all four-character is recommended. (e.g., 14 characters using a mix of all four-character sets in the first 7 character and the last characters).

(5) User Validation. User is required each time to log onto the system, either initially or after a screen lock program is interrupted. Then user is required to log off at end of the session.

(6) Password Protection

(a) Passwords must not be displayed at any terminal or printer.

(b) The user will employ appropriate actions to prevent disclosure while logging onto the system.

(c) Practice entry of the password so that it can be quickly entered.

(d) Shield the keyboard to prevent the observer from seeing the keys being pressed during password entry.

(e) Request a guest not watch the password entry process.

(f) Logon prior to demonstrating use of the system.

(7) User Maintenance. Passwords must be changed or invalidated by SA or NA at least every 90 days or less for classified systems (e.g., Secret Internet Protocol Router Network (SIPRNET) and for unclassified but sensitive controlled systems (e.g., Non-Secure Internet Protocol Router Network (NIPRNET). Organizations may consider shorter periods for user or SA/NA passwords on sensitive systems requiring greater security.

(8) Storage

(a) Passwords will be stored in the authentication system that minimizes their exposure to disclosure or unauthorized replacement.

(b) Encryption of electronic-stored passwords and password files is required.

(c) Passwords will never be part of the boot process or be executed via function keys.

(d) Password Vaults:

1. A password vault is a utility program that stores multiple passwords under a master password. This eliminates the problem of users forgetting multiple passwords or having to write them down.

2. The use of a password vault will only be considered if:

a. Passwords are stored by a minimum of 128-bit encryption.

b. The vendor provides a Vendor Integrity Statement.

c. The SA/NA or IM approves the software and use of this product is reflected in the system accreditation.

d. Default directory names will be changed to prevent easy targeting by automated password cracking programs.

c. Authentication Failures:

(1) Users will be allowed no more than three (3) attempts to log onto system. After the maximum number of attempts is exceeded, the account must be locked.

(2) If technically feasible, the system will also prevent rapid retries when a password is entered incorrectly. Several seconds should elapse before another password is requested. The system may also allow passwords to reset after a given amount of time (e.g., 15 minutes). This prevents an automated, high-speed Denial of Service (DOS) attack via account lockout on the password system.

(3) Ideally, the logon prompts will immediately go to the password prompt. If an unsuccessful logon has taken place, there will be no indication as to whether the logon USERID or password caused the failure.

(4) A security record will be maintained of the passwords entered incorrectly, but the incorrect password should not be kept in the record. A security alarm should be generated if:

(a) The maximum number of allowed account password retries is exceeded.

(b) The maximum number of allowed failed logons from one terminal is exceeded.

(c) The maximum number of allowed failed logons for a period is exceeded.

(5) The above security parameters must be set to the sensitivity of the data being protected, the profile of the typical system user, and the policy of the organization.

(6) User accounts will be disabled, and users should be denied service if these parameters are exceeded. The SA/NA should be the only one who can reset the account and restore the service of the user following these events.

(7) The system should inform the user, following a successful logon procedure, of the date and time of the last successful access by the user and any unsuccessful intervening access attempts. The notification should not scroll by but remain on the screen until another keystroke is entered giving the user a chance to view the statement. This will aid in

uncovering any unauthorized accesses or attempted accesses that may have occurred between authorized user accesses.

d. User Password History. A history of individual password usage will be maintained by SA/NA for 1 year to preclude the use of old passwords. Users or SA/NAs will not be able to reuse any of the last ten sets of previous passwords. If a password history is not available, the SA/NA should audit password activity to ensure that no individuals use any of their last ten sets of prior passwords.

e. Memorizing Passwords

(1) Users will memorize their passwords; however, if it is necessary to maintain a password list it must be kept secured.

(2) Users are encouraged not to keep a copy of their written password, but it is often necessary to have it available. The password should be protected as follows to prevent loss and to detect a compromise.

(a) Do not store the password where it is easily accessible near the computer.

(b) Do not keep the password and USERID together.

(c) Store the password in a locked drawer, cabinet, or container.

(d) Seal the password in an envelope and sign across the seal to detect tampering.

f. Disclosure of Passwords

(1) Users will not disclose their passwords to anyone.

(2) Disclosing a personal classified password to anyone without a valid clearance or need to know constitutes a security violation and will be dealt with appropriate personnel action by the CO or Section Manager.

(3) Disclosing an account password or permitting unauthorized use of a DOD computer system or network constitutes a security violation and will be dealt with appropriate personnel action by CO or section Manager. Authorization for computer network use may be obtained from SA/NA personnel, who were granted such authority by the DAA.

g. Compromised Passwords. Users must immediately notify the SA, NA or Information Manager (IM) if it is believed that a password has been compromised. Units not having an IM will notify the ACTR.

h. Unclassified System Access

(1) SA/NAs will not share unclassified system access passwords with other SA/NAs.

(2) Unclassified system access passwords maintained on paper will be sealed in a Standard Form 700 or plain envelope and protected.

i. Classified System Access

(1) SA/NAs will not make classified system passwords available to anyone, including other SA/NAs.

(2) Classified system access passwords maintained on paper will be sealed in a Standard Form 700 and stored in a secure container with access to those with a need to know.

j. Factory-Issued Identifiers or Passwords. All factory-set, defaults, or standard USERIDs and passwords will be removed and changed prior to the system going operational. Afterwards, systems will be rechecked periodically to confirm upgrades or patches have not reinstalled factory password defaults or other types of backdoors intrusion by unauthorized personnel.

k. Conditions Requiring Password Changes

(1) Passwords will be changed when compromised, possibly compromised, forgotten, or if suspicious activity on an account appears in an audit log.

(2) Group passwords are discouraged; however, in some watch-standing or administrative situations, DAAs may approve use conditionally. If a group password is authorized and created, the password must be changed when compromised or a member of the group leaves.

l. Disabling Accounts

(1) USERIDs will be removed or reassigned within 2 days of notification that a user no longer requires access to the system.

(2) Users and supervisors are responsible for notifying SA/NAs or Information Managers (IM)/Security Managers (SM) when access is no longer required.

(3) SA/NAs will suspend USERIDs and passwords that have not been used in a 90-day period.

(4) User accounts will be disabled immediately upon identification of unauthorized activity by user.

m. Classification and Control of Passwords

(1) All passwords of unclassified systems will be treated as sensitive and secured appropriately.

(2) Passwords of classified systems will be classified at the accredited classification level of the system and secured appropriately.

6. Responsibility. CNATRA CIO is the official approval authority for Information Management and Information Technology (IMIT), which include operations and support of Information Systems (IS) for CNATRA and NATRACOM units. All support actions and documentations relative to IS administration will be channeled and coordinated through the respective chain, the Activity Customer Technical Representative (ACTR), then to the CNATRA CIO office. Unit Commanding Officers will implement this policy, administration, guidelines and procedures within their commands.

7. Contact Information for CNATRA CIO: CNATRA (N6), (R
250 Lexington Boulevard, Suite 102, Corpus Christi, TX 78419-5041, DSN 861-1430 or Commercial (361) 961-1430.

D. B. Grimland

D. B. GRIMLAND
Chief of Staff

Distribution:
CNATRAINST 5215.1R
List I
List III

Copy to:
COMTRAWING TWO (Coop File)
NETC

BLANK PAGE

WEB LINKS TO REFERENCES

CJSCM 6510.01 is FOR OFFICIAL USE ONLY (FOUO) DOCUMENT and is available at the INFOSEC web site. Click on "Documentation" link, on respective document number. Refresh page, if necessary, to view page.
https://infosec.navy.mil

DODD 8500.1
http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf

DODI 8500.2
http://www.dtic.mil/whs/directives/corres/pdf/i85002_020603/i85002p.pdf

DODI 5200.40 (rev July 24, 2003) DITSCAP
http://www.dtic.mil/whs/directives/corres/pdf/i520040_123097/i520040p.pdf

DODD 8000.1
http://www.dtic.mil/whs/directives/corres/pdf/d80001wch1_022702/d80001p.pdf

CNATRAINST 5000.2C CNATRA CIO Mission, Functions and Policy (R
https://cnatra.navaltx.navy.mil/cnatra/instruct.htm

CNATRAINST 5200.7B Naval Air Training Information Assurance (IA) Program (R
https://cnatra.navaltx.navy.mil/cnatra/instruct.htm

OPNAVINST 5239.1b
http://neds.nebt.daps.mil/Directives/5239_1b.pdf